МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА НАЦІОНАЛЬНОГО, МІЖНАРОДНОГО ПРАВА
ТА
ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

КІБЕРЗЛОЧИННІСТЬ ТА ВИКЛИКИ КІБЕРБЕЗПЕКИ ДЛЯ ПРАВООХОРОННИХ ОРГАНІВ

Кваліфікаційна робота (проєкт)

на здобуття ступеня вищої освіти «магістр»

Виконав: студент ІІ курсу 10-283 М група
Спеціальності:
262 “Правоохоронна діяльність”
Освітньо-професійної програми «Правоохоронна діяльність»
Хрустальов Антон Сергійович

Керівник **к.ю.н., доц. Гладенко О.М.**

Рецензент **д.ю.н., проф. Шкута О.О.**

Івано-Франківськ – 2024

ЗМІСТ

ВСТУП

Актуальність теми дослідження кіберзлочинності та викликів кібербезпеки для правоохоронних органів обумовлена стрімким розвитком цифрових технологій, який, з одного боку, надає нові можливості для суспільства, а з іншого — створює численні загрози. Сучасні інформаційні системи, інтернет і соціальні мережі стали невід'ємною частиною життя як громадян, так і державних органів, забезпечуючи оперативну комунікацію, передачу даних та доступ до інформації. Разом із цим зросла кількість кіберзлочинів, які мають складну структуру, важкі наслідки та вимагають значних ресурсів для розслідування й протидії.

Кіберзлочинність стає глобальною проблемою, оскільки відсутність чітких національних кордонів у цифровому просторі ускладнює притягнення винних до відповідальності. Кіберзлочини, такі як хакерські атаки, фішинг, фінансове шахрайство, поширення шкідливого програмного забезпечення та інші злочинні дії, створюють загрозу для національної безпеки та приватного сектора. Це особливо важливо в контексті зростаючої залежності державних і приватних структур від інформаційних технологій, що робить їх більш уразливими для атак.

З огляду на вищезазначене, дослідження кіберзлочинності та заходів протидії кіберзагрозам має велике значення для розвитку ефективної системи захисту правоохоронних органів та держави загалом.

Зв'язок роботи з науковими програмами, планами, темами. Кваліфікаційна робота пов'язана з науковими програмами та планами, спрямованими на підвищення рівня національної безпеки та кіберстійкості держави. Зокрема, робота відповідає актуальним завданням Державної програми кібербезпеки, що передбачає посилення захисту інформаційних ресурсів і боротьбу з кіберзлочинністю. Дослідження також узгоджується з науковими темами, пов'язаними з розвитком інноваційних технологій у правоохоронній діяльності, зокрема в аспекті захисту державних установ від

кібератак та підвищення ефективності протидії злочинності у цифровому просторі.

Метою роботи є дослідження кіберзлочинності та визначення ефективних заходів кібербезпеки для підвищення здатності правоохоронних органів протидіяти сучасним кіберзагрозам.

Відповідно до поставленої мети, нами будуть виконані наступні ***завдання:***

- охарактеризувати поняття кіберзлочинності та її різновиди;
- визначити основні методи та засоби, що використовуються в кіберзлочинності;
- проаналізувати кіберзлочинність у міжнародному праві та національних системах законодавства;
- дослідити сучасні загрози кібербезпеці та їх вплив на діяльність правоохоронних органів;
- виокремити методи та засоби захисту від кіберзлочинності: міжнародний досвід і практика в Україні;
- визначити перспективи та проблеми використання новітніх технологій у протидії кіберзлочинності.

Об'єктом дослідження є процеси протидії кіберзлочинності та забезпечення кібербезпеки в діяльності правоохоронних органів.

Предметом дослідження є методи та засоби кібербезпеки, які використовуються правоохоронними органами для запобігання та протидії кіберзлочинності.

Методи дослідження. Для досягнення поставленої мети в роботі використано комплекс методів дослідження. Зокрема, метод аналізу і синтезу допоміг розглянути теоретичні основи кіберзлочинності та особливості кіберзагроз для правоохоронних органів. Порівняльний метод застосовувався для аналізу міжнародного досвіду у сфері кібербезпеки та визначення

найефективніших практик протидії кіберзлочинності. Статистичний метод дозволив оцінити масштаби кіберзлочинності на основі наявних даних. Також використовувалися методи системного підходу та експертного оцінювання для узагальнення результатів дослідження та формулювання практичних рекомендацій.

Наукова новизна одержаних результатів полягає у визначенні специфічних сучасних загроз кібербезпеці, з якими стикаються правоохоронні органи, та розробці рекомендацій щодо використання новітніх технологій у протидії кіберзлочинності. Вперше систематизовано методи та інструменти, які можуть підвищити ефективність виявлення й розслідування кіберзлочинів, а також запропоновано модель інтеграції міжнародних стандартів кібербезпеки у національну систему правоохоронної діяльності. Отримані результати доповнюють наукову базу щодо забезпечення кіберстійкості державних структур і можуть бути використані для вдосконалення правових та організаційних підходів до протидії кіберзагрозам.

Практичне значення одержаних результатів полягає в їхній застосовності для підвищення ефективності роботи правоохоронних органів у сфері кібербезпеки. Розроблені рекомендації щодо впровадження новітніх технологій, удосконалення методів виявлення та розслідування кіберзлочинів можуть бути використані для навчання кадрів, оптимізації оперативної діяльності та формування стратегій реагування на кіберзагрози. Отримані результати також можуть слугувати основою для розробки політик та нормативно-правових актів у сфері кібербезпеки, що сприятиме поліпшенню співпраці між правоохоронними органами та міжнародними організаціями. Впровадження запропонованих підходів дозволить знизити ризики кіберзлочинності, підвищити рівень безпеки інформаційних систем та захистити державні та приватні інтереси в умовах зростаючої цифровізації.

Структура. Кваліфікаційна (магістерська) робота складається зі вступу, двох розділів, висновків та списку використаних джерел (43 найменування). Загальний обсяг роботи становить 55 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНА ХАРАКТЕРИСТИКА ТА ОСОБЛИВОСТІ КІБЕРЗЛОЧИННОСТІ

1.1. Поняття кіберзлочинності та її різновиди

Кіберзлочинність є одним із найактуальніших викликів сучасного суспільства, який вимагає комплексного осмислення, дослідження та розробки ефективних засобів захисту. З розвитком цифрових технологій злочинці почали активно використовувати комп'ютерні мережі та пристрої для досягнення своїх протиправних цілей. Із цього моменту з'явилося поняття кіберзлочинності, яке охоплює величезну кількість різновидів злочинної діяльності, здійснюваної в інформаційному просторі. Саме це розмаїття та багатогранність вимагають детального аналізу для розуміння, як і чому кіберзлочини стали такими поширеними й небезпечними.

Загалом, кіберзлочинність охоплює незаконні дії, пов'язані з використанням комп'ютерних систем, мереж або пристроїв. Це не просто результат технологічних змін, а новий спосіб здійснення злочинів, що має певні особливості та виклики для традиційних правових систем. Злочинці, які використовують цифрові технології, відрізняються від звичайних тим, що можуть перебувати в будь-якій точці світу, залишаючись при цьому анонімними, а також володіють високими технічними знаннями. Тому кіберзлочинність часто виглядає більш непередбачуваною та небезпечною, аніж традиційні види злочинів [1, с.163].

Сучасна кіберзлочинність включає в себе різні форми незаконної діяльності, які виходять за межі звичайного порушення прав користувачів. Це не лише традиційні форми обману, як шахрайство чи крадіжка особистих даних, але й більш складні види атак, як-от кібершпигунство або саботаж критично важливої інфраструктури. Відповідно до свого підходу до злочину, кіберзлочини можна розділити на кілька основних видів, таких як хакерство,

поширення шкідливого програмного забезпечення, кібертероризм та інші, проте кожен із них має свої особливості та цілі.

Хакерство – це один із найпоширеніших видів кіберзлочинів, який передбачає проникнення до системи чи мережі без дозволу з метою отримання або зміни даних. Зловмисники, що здійснюють хакерські атаки, можуть мати різні цілі, починаючи від бажання отримати конфіденційну інформацію та закінчуючи нанесенням шкоди репутації чи фінансових збитків. Часто вони використовують спеціальні методи, такі як злом паролів або соціальна інженерія, щоб отримати доступ до даних [1, с.170].

Соціальна інженерія, як метод, що тісно пов'язаний із хакерством, має на меті психологічно вплинути на людей, змусивши їх добровільно надати доступ до важливих даних чи систем. В цьому випадку кіберзлочинці не тільки покладаються на технічні засоби, а й використовують людські емоції та довіру. Соціальна інженерія може мати різні форми, від простих обманів до ретельно спланованих сценаріїв, де злочинці видають себе за іншу особу або організацію.

Окремим важливим видом кіберзлочинності є поширення шкідливого програмного забезпечення (malware). Шкідливі програми створюються з метою заподіяння шкоди комп'ютерам, отримання доступу до них або крадіжки інформації. Віруси, троянські програми, шпигунське ПЗ – усе це різновиди шкідливого програмного забезпечення, яке використовується для нанесення збитків як окремим користувачам, так і великим організаціям. У деяких випадках шкідливе ПЗ може блокувати системи, що викликає фінансові та репутаційні втрати [2, с.16].

Фінансові шахрайства також входять до сфери кіберзлочинності, охоплюючи незаконні дії з фінансовими ресурсами, такими як крадіжка банківських даних або онлайн-шахрайство з кредитними картками. Цей вид злочину є особливо поширеним через можливість легко отримати доступ до банківських рахунків, часто за допомогою фішингових сайтів або електронних

листів, які мають на меті обманути користувача, змусивши його розкрити свої облікові дані.

Фішинг – це ще один розповсюджений метод кіберзлочинців, який спрямований на обман користувачів і отримання їхньої особистої інформації шляхом створення фальшивих сайтів або електронних повідомлень, що виглядають як справжні. Злочинці користуються тим, що багато людей не відразу можуть відрізнити фальшивий сайт від справжнього, тому фішинг залишається ефективним інструментом [3, с.95].

Кібертероризм представляє собою надзвичайно небезпечну форму кіберзлочинності, яка переслідує політичні або ідеологічні цілі. У таких випадках злочинці не просто намагаються отримати вигоду або доступ до інформації, а прагнуть дестабілізувати ситуацію в країні чи зруйнувати важливу інфраструктуру. Кібертерористи можуть атакувати урядові установи, банки, об'єкти енергетики, що може призвести до серйозних наслідків для суспільства.

Кібершпигунство – це небезпечний вид злочинної діяльності, який має на меті збір конфіденційної інформації про компанії, організації чи держави для отримання конкурентних переваг або проведення розвідки. У сучасному світі, де інформація стає одним з найцінніших ресурсів, кібершпигунство перетворюється на важливий інструмент не лише для бізнесу, але й для урядів. Конфіденційні дані, такі як розробки нових продуктів, стратегії ринку, фінансова інформація та персональні дані клієнтів, можуть мати величезну цінність на чорному ринку або ж бути використані для підриву конкурентів [4, с.145].

Атаки кібершпигунства часто здійснюються за допомогою шкідливого програмного забезпечення, яке може включати віруси, трояни та шпигунські програми. Зловмисники використовують різноманітні методи для прихованого збору даних, такі як фішингові листи, соціальна інженерія або навіть фізичний доступ до обладнання. Однією з поширених тактик є встановлення шпигунського ПЗ на комп'ютери жертв, що дозволяє отримувати

доступ до електронних листів, файлів та комунікацій без відома користувача. Оскільки такі дії часто залишаються непоміченими, жертви можуть тривалий час не усвідомлювати, що їхні дані знаходяться під загрозою.

З розвитком технологій та збільшенням кількості даних, які компанії генерують щодня, кібершпигунство стає все більш актуальним. Багато великих корпорацій інвестують у кібербезпеку, але навіть найсучасніші системи можуть бути вразливими до добре спланованих атак. Зловмисники постійно вдосконалюють свої методи, щоб обходити заходи безпеки, і в умовах глобалізації інформаційних технологій, кібершпигунство набуває транснаціонального характеру [5, с.198].

Ця ситуація викликає серйозні занепокоєння, оскільки витоки конфіденційних даних можуть призвести не лише до фінансових втрат, а й до пошкодження репутації, втрати довіри з боку клієнтів і партнерів, а також до правових наслідків. У результаті, бізнесам важливо не лише вжити заходів для захисту своїх даних, але й виховувати культуру обізнаності серед працівників щодо кібербезпеки, адже людина є часто найслабшою ланкою у системі захисту. Загалом, кібершпигунство підкреслює необхідність комплексного підходу до захисту інформації в умовах зростаючої цифрової загрози.

Додатково слід виділити кібербулінг, що є формою кіберзлочинності, яка здебільшого стосується окремих користувачів. Кібербулінг полягає у психологічному тиску, переслідуванні, або ж дискримінації особи за допомогою цифрових платформ, часто в соціальних мережах. Цей вид злочинності стає дедалі більш поширеним, особливо серед молоді, і викликає серйозні соціальні проблеми [6, с.18].

Ще одним небезпечним різновидом кіберзлочинності є атаки на критичну інфраструктуру, як-от електромережі, водопостачання або транспорт. Метою таких атак є виведення з ладу життєво важливих об'єктів, що може мати катастрофічні наслідки для населення. Зловмисники часто вибирають такі об'єкти через їхню високу вразливість і стратегічну значущість.

Також існують випадки кіберзлочинності, які пов’язані з порушенням інтелектуальної власності, зокрема нелегальне копіювання чи розповсюдження захищених матеріалів, таких як музика, фільми, книги або програмне забезпечення. Інтернет-піратство шкодить творцям контенту та власникам авторських прав, тому розглядається як серйозний вид порушення.

Загалом, кіберзлочинність не має чітко окреслених кордонів і може набувати різних форм. З розвитком нових технологій і збільшенням кількості користувачів інтернету її масштаби лише зростають. У кожного з різновидів кіберзлочинності є свої методи, технічні особливості, а також мотиви, що їх керують. Тому для ефективного протистояння кіберзлочинам необхідний комплексний підхід, який охоплює як технічні, так і соціальні аспекти.

Однією з ключових проблем кіберзлочинності є її швидка еволюція. Злочинці постійно адаптуються до нових систем захисту, розробляючи нові методи для обходу безпеки. Таким чином, навіть сучасні системи захисту не можуть гарантувати повної безпеки, оскільки злочинці завжди шукають нові шляхи проникнення. Це породжує своєрідну гонку озброєнь між злочинцями та розробниками засобів кібербезпеки [6, с.20].

Розмаїття видів кіберзлочинності свідчить про те, що для її подолання потрібна не лише технічна, але й правова підготовка. Закони мають адаптуватися до швидких змін у цифровій сфері, що часто виявляється важким завданням для правової системи. Окрім того, міжнародна співпраця є невід'ємною складовою успішної боротьби з кіберзлочинністю, оскільки злочинці можуть діяти з території будь-якої країни.

У сучасних умовах кіберзлочинність є не лише проблемою для окремих компаній чи користувачів, а й серйозною загрозою для держав. Випадки кібератак на урядові системи, виборчі процеси та інфраструктуру свідчать про те, що кіберзлочинці стають усе більш організованими й небезпечними, а їхні дії можуть мати політичний підтекст.

Таким чином, кіберзлочинність постає перед нами не лише як загроза для особистої безпеки чи фінансових активів, а й як масштабне суспільне явище, що впливає на всі аспекти життя.

1.2. Основні методи та засоби, що використовуються в кіберзлочинності

Кіберзлочинність охоплює широкий спектр загроз, що мають значний вплив на інформаційну безпеку організацій, приватних осіб та національних структур. Сучасні кіберзлочинці використовують численні методи і техніки, що постійно розвиваються, адаптуючись до нових технологій і вдосконалюючись у відповідь на кіберзахист. Серед основних методів кіберзлочинності сьогодні варто виділити атаки зловмисного програмного забезпечення, фішинг, соціальну інженерію, DDoS-атаки та складні методи проникнення в системи за допомогою експлойтів і вразливостей. Кожен із цих методів має унікальні характеристики і тактики, які використовуються кіберзлочинцями з різними цілями та мотивами.

Зловмисне програмне забезпечення (malware) – це невидимий ворог сучасного цифрового світу, що проникає в системи, щоб викрасти, пошкодити або блокувати інформацію користувача. Воно здатне обманом пробратися в пристрій, використовуючи слабкі місця системи, уразливості програмного забезпечення або довірливість користувачів. Віруси, трояни, шпигунські програми, програми-вимагачі й руткіти представляють різні типи цього шкідливого ПЗ, але всі вони мають спільну мету – використати пристрій жертви у власних цілях. Деякі з них налаштовані на завдання незначної шкоди, інші ж здатні завдати серйозних руйнувань, спричиняючи втрату особистої інформації або навіть фінансових ресурсів [7, с.167].

Трояни – один із найпоширеніших методів зловмисного проникнення. Цей тип ПЗ відомий здатністю маскуватися під безпечні файли, документи чи програми. Наприклад, троян може виглядати як звичайне оновлення системи

або як популярна програма, яку користувач бажає встановити. Після відкриття або встановлення троян запускається у фоновому режимі, надаючи зловмиснику прихований доступ до пристрою. Це дозволяє викрасти дані, отримати паролі або здійснювати інші маніпуляції з пристроєм без відома жертви. Завдяки такому доступу, зловмисники можуть не лише красти інформацію, а й використовувати пристрій для нових кібератак або навіть шантажу власника.

Програми-вимагачі, з іншого боку, здатні блокувати доступ до файлів чи системи, поки жертва не виплатить викуп. Вони можуть проникнути на пристрій через заражені електронні листи, сумнівні посилання або інші способи соціальної інженерії. Після активації ці програми шифрують дані жертви або обмежують доступ до них, вимагаючи виплати за розблокування. Враховуючи, що ці загрози здатні призвести до значних втрат для як приватних осіб, так і великих компаній, важливість кібербезпеки та використання антивірусного захисту стає особливо актуальною [8, с.60].

Руткіти – ще одна потужна загроза, оскільки дозволяють зловмисникам глибоко приховати своє ПЗ у системі, роблячи його непомітним для стандартних заходів безпеки. Руткіти діють на рівні ядра операційної системи, що робить їх вкрай важкими для виявлення. Вони можуть використовуватися для отримання глибокого контролю над системою, що відкриває зловмисникам можливість змінювати налаштування, видаляти чи додавати файли, записувати дії користувача.

Програми-вимагачі особливо небезпечні для компаній та державних організацій, оскільки вони здатні блокувати доступ до всієї критично важливої інформації, вимагаючи викуп. Ця категорія зловмисного ПЗ може завдати значних фінансових збитків, а іноді призводить до повного паралічу роботи організацій. Ця атака відбувається через зараження пристрою програмою, що шифрує файли, і навіть при відновленні частини системи компанії часто стикаються зі значною втратою даних і часу [9, с.330].

Фішинг є одним із найпоширеніших і водночас найефективніших методів кіберзлочинності, оскільки використовує людський фактор, а не тільки технічні вразливості систем. Основною метою фішингових атак є обман користувача з метою викрадення його конфіденційної інформації, такої як паролі, номери банківських карток, паспортні дані та інші персональні відомості. Часто фішингові атаки виглядають цілком легітимно, оскільки зловмисники приділяють особливу увагу імітації відомих компаній, банків або державних установ, аби викликати у жертви відчуття довіри.

Одним із найбільш поширених прийомів є фішингові електронні листи, які надходять користувачам нібито від банків або популярних онлайн-сервісів. У цих листах часто містяться прохання підтвердити особисті дані, оновити інформацію безпеки чи навіть виконати екстрені дії задля безпеки облікового запису. Листи можуть бути написані в терміновому тоні, з використанням емоційного тиску, щоб користувач відчував необхідність негайно виконати вимоги. Наприклад, повідомлення про нібито несанкціонований доступ або підозрілу активність стимулюють людей вводити свої паролі або інші дані на підроблених сторінках. Такі веб-сайти можуть виглядати майже ідентично з оригіналом, що ускладнює їх відрізнення для пересічного користувача [10, с.261].

Фішинг є небезпечним через його здатність проникати до фінансової або особистої інформації, використовуючи мінімальну взаємодію із системою захисту. Кіберзлочинці, які отримали доступ до інформації жертви, можуть скористатися нею для прямих крадіжок, перепродажу даних на чорному ринку або навіть для створення нових, більш масштабних схем шахрайства. Фішинг також еволюціонує: зокрема, він адаптується до нових платформ, соціальних мереж і месенджерів, а також створює персоналізовані атаки, які вимагають складніших методів виявлення.

Ця підступність і гнучкість фішингу змушують компанії інвестувати в освітні програми для своїх працівників, аби мінімізувати ризики. Користувачам рекомендується дотримуватися простих правил кібергігієни,

наприклад, уважно перевіряти адреси електронної пошти та веб-сайтів, не відкривати сумнівні посилання та бути скептичними до запитів на конфіденційну інформацію. Тільки поєднання технічного захисту і підвищеної обізнаності користувачів може ефективно протистояти фішинговим атакам, що залишаються важливою загрозою в сучасному кіберсвіті [11, с.128].

Окрему роль у кіберзлочинності відіграє соціальна інженерія, що базується на психологічному впливі на жертву. Кіберзлочинці часто використовують техніки соціальної інженерії, щоб переконати користувачів надати доступ до систем або інформації, використовуючи маніпуляції, обман чи загрозу. Наприклад, атакуючі можуть видати себе за співробітників служби техпідтримки, аби отримати паролі чи інші доступи до облікових записів жертви. Соціальна інженерія є особливо небезпечною, оскільки вона обходить технічні засоби захисту і зосереджується на слабкостях людини.

DDoS-атаки (розподілені атаки на відмову в обслуговуванні) є одним із найпотужніших інструментів кіберзлочинців, який використовується для тимчасового виведення з ладу веб-сайтів, серверів чи онлайн-платформ шляхом перевантаження їхнього трафіку. Ці атаки реалізуються через масове і одночасне надсилання запитів до цільового ресурсу з багатьох різних пристроїв, об’єднаних у так звані ботнети. Величезна кількість запитів призводить до того, що сервери не можуть обробити їх усі й, зрештою, починають працювати повільно або зовсім перестають реагувати. Як наслідок, справжні користувачі не можуть отримати доступ до сервісу, а бізнеси несуть збитки через недоступність своїх онлайн-ресурсів [12, с.96].

Мотиви DDoS-атак можуть бути різними, але часто вони стають інструментом шантажу: зловмисники загрожують здійснити або продовжувати атаку, вимагаючи викуп для відновлення нормальної роботи. Для бізнесів, чия діяльність залежить від безперервної онлайн-роботи, наприклад, для інтернет-магазинів, банківських установ або новинних ресурсів, такі атаки можуть призвести до значних фінансових та репутаційних втрат. В умовах сучасної цифрової економіки навіть кілька хвилин простою

можуть обернутися мільйонними збитками, що часто змушує жертв DDoS-атак поступатися вимогам кіберзлочинців.

У багатьох випадках зловмисники використовують ботнети, створені з інфікованих пристроїв, зокрема комп'ютерів, роутерів, смартфонів, що несвідомо беруть участь у таких атаках. Через це власники цих пристроїв можуть навіть не підозрювати, що вони використовуються для DDoS-атаки, що ускладнює їхнє виявлення та блокування. Ботнети дозволяють зловмисникам надсилати мільйони запитів за секунду, створюючи лавиноподібне навантаження на цільову систему. Оскільки джерела атак розподілені по всьому світу, захист від них потребує комплексного підходу: від фільтрації підозрілого трафіку до блокування певних IP-адрес і автоматизованих засобів для виявлення аномальної активності [13, с.184].

Сьогодні кібербезпека активно розвиває засоби протидії DDoS-атакам, однак вони все ще залишаються серйозною загрозою. Технічні рішення, такі як мережі для доставки контенту (CDN), використання проксі-серверів та розширені системи моніторингу, допомагають пом'якшити наслідки атак, але повністю уникнути цієї загрози практично неможливо. Оскільки технології вдосконалюються, зловмисники також знаходять нові способи оптимізації своїх атак, що робить боротьбу з DDoS безперервною гонкою між атакуючими та захисниками.

Кібершахрайство включає ще одну категорію загроз, що використовуються для фінансового викрадення коштів або обману користувачів. Наприклад, шахраї можуть створювати підроблені інтернет-магазини або сайти, де користувачі вводять дані своїх карток, які згодом використовуються для несанкціонованих покупок. Цей вид кіберзлочинності набирає популярності завдяки активному розвитку онлайн-торгівлі, яка забезпечує шахраям широкі можливості для маніпуляцій і обману покупців [14].

Також важливу роль у кіберзлочинності відіграють експлойти – спеціальні програми або скрипти, що використовують уразливості у

програмному забезпеченні для отримання несанкціонованого доступу до систем. Часто, коли виявляється нова уразливість, кіберзлочинці швидко використовують її для створення експлойтів, які дозволяють проникати в системи та викрадати дані. Такі атаки часто проводяться на великі організації, де навіть невеликі уразливості можуть призвести до значних втрат [15].

Боти і бот-мережі використовуються зловмисниками для здійснення атак на велику кількість пристроїв одночасно. Ботнети – це мережі заражених пристроїв, що під контролем кіберзлочинців виконують команди для масового розсилання спаму, запуску DDoS-атак або навіть виконання складних обчислень для криптомайнінгу. Бот-мережі можуть складатися з тисяч і навіть мільйонів пристроїв, що робить їх надзвичайно потужним інструментом у руках кіберзлочинців.

Використання криптовалют для фінансування кіберзлочинної діяльності стало новою тенденцією. Завдяки анонімності, криптовалюти дозволяють кіберзлочинцям отримувати викупи, зберігаючи конфіденційність. Наприклад, у випадках з програмами-вимагачами кіберзлочинці часто вимагають сплату викупу в біткоїнах або інших криптовалютах, що ускладнює відстеження транзакцій і ідентифікацію зловмисників [16, с.152].

Розвиток технологій, таких як Інтернет речей (IoT), також створює нові вразливості, які можуть бути використані кіберзлочинцями. Пристрої IoT, зазвичай, мають недостатній рівень безпеки, і зловмисники можуть використовувати їх для атак на більш великі мережі або як частину ботнетів. Наприклад, через несанкціонований доступ до розумних камер спостереження чи термостатів кіберзлочинці можуть не тільки викрасти дані, але й отримати фізичний контроль над об'єктами.

Один з новітніх методів у кіберзлочинності – це атаки на основі штучного інтелекту (ШІ). Кіберзлочинці почали використовувати ШІ для автоматизації атак, що дозволяє їм проводити атаки швидше і з більшою точністю. Наприклад, алгоритми ШІ можуть автоматично визначати слабкі

місця в системах або навіть створювати фальшиві зображення та відео для дезінформаційних кампаній [17, с.73].

Також важливим компонентом є крадіжка особистих даних, яка може бути здійснена як за допомогою фішингових атак, так і через зламані бази даних. Здобуті дані, такі як номери соціальних страхувань, медичні записи або фінансові дані, можуть бути використані для подальшого шахрайства або продані на чорному ринку.

Атакуючі активно використовують методи маніпуляції мережевим трафіком, такі як атаки «людина посередині», що дозволяють перехоплювати комунікації між користувачем і веб-сайтом. Ці атаки можуть здійснюватися як у публічних Wi-Fi мережах, так і через уразливості в захищених з'єднаннях, надаючи кіберзлочинцям доступ до даних, що передаються.

Крім цього, зловмисники використовують методи шифрування для маскування своєї діяльності. Наприклад, для приховування свого трафіку вони можуть використовувати VPN або анонімні мережі, такі як Tor. Це ускладнює спроби відстеження їхньої діяльності та забезпечує додатковий рівень безпеки, який перешкоджає розкриттю їхньої особи.

Боротьба з кіберзлочинністю потребує комплексного підходу і активної співпраці на рівні держав, організацій та приватних осіб. Спеціальні підрозділи кіберполіції, антивірусні компанії та експерти з безпеки постійно працюють над розробкою нових методів захисту, однак складність і динамічний розвиток кіберзлочинних методів роблять цю боротьбу постійною та непередбачуваною [18, с.19].

На закінчення, кіберзлочинці постійно адаптуються, використовуючи найсучасніші технології та методи для досягнення своїх цілей. Знання про методи кіберзлочинності дозволяє більш ефективно захищати інформацію та підвищує обізнаність користувачів, які часто стають першою лінією захисту від таких загроз.

1.3. Кіберзлочинність у міжнародному праві та національних системах законодавства

Кіберзлочинність стала однією з головних загроз сучасності, викликом, що охоплює широкий спектр правових, технологічних, соціальних та політичних аспектів. В умовах глобалізації та розвитку інформаційних технологій, коли цифрові системи глибоко інтегровані у всі сфери життя, кіберзлочинність вражає як окремих користувачів, так і уряди, міжнародні корпорації та національні економіки в цілому. Поширеність кібератак, інцидентів витоку даних, фішингових схем та інших видів кіберзлочинів спонукає до розробки ефективних механізмів запобігання, моніторингу та реагування на кіберзагрози, однак їх практична реалізація є непростим завданням, зважаючи на правові, технічні та культурні розбіжності між державами.

Міжнародне право, що є основою для співпраці держав у сфері кібербезпеки, поки що не виробило єдиної конвенції чи закону, який би врегульовував усі аспекти кіберзлочинності. На цей момент більшість норм міжнародного права стосуються традиційних форм злочинів, не враховуючи специфіку кіберзагроз, які не мають фізичних меж і можуть впливати на інтереси багатьох країн одночасно. У цих умовах окремі країни змушені самостійно адаптувати своє законодавство до умов цифрової епохи, що призводить до фрагментарності у підходах до регулювання кіберзлочинності [19].

Одним із перших і найважливіших документів у сфері міжнародного правового регулювання кіберзлочинності стала Будапештська конвенція Ради Європи про кіберзлочинність, прийнята у 2001 році. Ця конвенція залишається єдиною міжнародною угодою, що покликана створити загальні правові стандарти боротьби з кіберзлочинами. Вона визначає основні види злочинів у сфері інформаційних технологій, зокрема доступ до комп'ютерних систем без дозволу, перехоплення даних, втручання у роботу систем і програм, а також

злочини, пов'язані з дитячою порнографією, фальшуванням та шахрайством. Країни-учасниці, серед яких і Україна, взяли на себе зобов’язання адаптувати свої національні законодавства відповідно до вимог конвенції.

Будапештська конвенція відіграє значну роль у гармонізації національних законодавств різних країн щодо боротьби з кіберзлочинністю. У рамках цієї конвенції створено механізм міжнародної співпраці, що включає обмін інформацією та допомогу у проведенні розслідувань між країнами-учасницями. Проте конвенція має певні обмеження: вона була розроблена понад два десятиліття тому, і її положення вже не враховують сучасних форм кіберзлочинів, таких як атаки на критичну інфраструктуру, масштабне викрадення особистих даних та криптовалюта як новий інструмент злочинної діяльності [20].

Незважаючи на важливість Будапештської конвенції, деякі країни, зокрема Росія, Китай та кілька інших держав, не є її підписантами. Вони висловлюють занепокоєння, що конвенція сприяє домінуванню західних стандартів у кібербезпеці та може використовуватися для впливу на національні інтереси. У зв'язку з цим деякі країни працюють над створенням альтернативного правового регулювання, яке враховуватиме їхні національні пріоритети та підходи до суверенітету в кіберпросторі.

У рамках Організації Об’єднаних Націй вже тривалий час тривають дискусії щодо створення єдиної угоди з кібербезпеки. Основними питаннями в цьому процесі є визначення чітких меж застосування міжнародного права в кіберпросторі, обов’язки держав щодо запобігання кібератакам та обмін інформацією про загрози. Проте через розбіжності в інтересах, підходах до прав людини та кіберсуверенітету країни ООН поки що не дійшли згоди щодо таких фундаментальних положень угоди [21].

У національних системах законодавства світу можна спостерігати різноманітні підходи до кіберзлочинності, що зумовлено як культурними, так і політичними особливостями кожної країни. Сполучені Штати Америки мають одну з найдетальніших і найсистематизованіших законодавчих баз, що

регулюють питання кібербезпеки. Одним із основоположних документів є Закон про комп'ютерне шахрайство і зловживання, прийнятий у 1986 році. Цей закон визначає кримінальну відповідальність за несанкціонований доступ до комп'ютерних систем, а також за використання комп'ютерів для шахрайства чи іншої злочинної діяльності. Таке законодавство стало основою для боротьби з кіберзлочинністю в США, встановлюючи чіткі рамки та відповідальність для правопорушників.

Крім того, існують й інші важливі закони, які підтримують цю структуру. Наприклад, Закон про захист інформації надає основи для регулювання захисту персональних даних та конфіденційної інформації, забезпечуючи більшу безпеку для громадян та організацій. Закон про кібербезпеку встановлює рамки для захисту критичної інфраструктури, моніторингу загроз, а також обміну інформацією між державними установами та приватними компаніями. Це сприяє створенню ефективної системи реагування на кіберзагрози та інтеграції зусиль усіх зацікавлених сторін у боротьбі з кіберзлочинністю [22].

Цей комплексний підхід, заснований на чітких законах та нормах, дозволяє Сполученим Штатам адаптуватися до швидко змінюваного технологічного середовища та нових викликів у сфері кібербезпеки. Проте варто зазначити, що такий рівень законодавчої деталізації і системності вимагає значних зусиль та ресурсів для імплементації, що може бути викликом для країн з обмеженими можливостями. У випадку України, важливо вивчити досвід США, щоб розробити власну адаптовану модель законодавства, яка враховувала б специфіку національних потреб і викликів. Це допоможе створити більш ефективну систему протидії кіберзлочинності, яка забезпечить безпеку держави та її громадян у цифрову еру.

Європейський Союз активно працює над створенням законодавчої бази, яка сприяє захисту даних та запобіганню кіберзлочинності. Одним із найважливіших нормативно-правових актів у цій сфері є Загальний регламент захисту даних (GDPR), який було прийнято в 2016 році. Цей регламент

встановлює суворі вимоги до захисту персональних даних, значно підвищуючи відповідальність компаній у питаннях кібербезпеки. Впровадження GDPR зобов'язує організації вживати заходів для захисту даних користувачів, забезпечуючи їхній конфіденційний статус та надаючи їм більше контролю над власними даними. Це не лише зменшує ризики порушення конфіденційності, але й підвищує рівень довіри споживачів до бізнесу [23, с.17].

Окрім GDPR, Європейський Союз також запровадив Директиву NIS2, яка зосереджена на захисті критичної інформаційної інфраструктури. Ця директива зобов'язує країни-учасниці забезпечувати надійний рівень кібербезпеки в важливих секторах економіки, таких як енергетика, транспорт, охорона здоров'я та цифрова інфраструктура. Директива NIS2 встановлює вимоги до виявлення, реагування на кіберінциденти та обміну інформацією між державними органами та приватними компаніями. Це створює основу для злагодженої роботи в боротьбі з кіберзлочинністю та загрозами, що виходять за межі національних кордонів.

У країнах Азії, таких як Китай і Південна Корея, можна спостерігати суттєві відмінності в підходах до законодавства у сфері кіберзлочинності, які зумовлені культурними, соціальними та політичними контекстами.

У Китаї законодавство характеризується суворим контролем за інформаційними системами та моніторингом інтернет-трафіку. Китайські закони, зокрема Закон про кібербезпеку, встановлюють жорсткі вимоги до компаній, які працюють в Інтернеті, зобов'язуючи їх забезпечувати контроль над інформаційними потоками та виявляти потенційні загрози. Це супроводжується серйозними покараннями за кібератаки та інші порушення, що дозволяє державі утримувати контроль над ситуацією у кіберпросторі. Однак, такий підхід також має свої недоліки, оскільки він значно обмежує приватність і права користувачів. Багато людей у Китаї стикаються з цензурою та обмеженнями в доступі до інформації, що викликає побоювання щодо порушення прав людини та свобод громадян.

На відміну від цього, Південна Корея в своєму законодавстві акцентує увагу на захисті персональних даних та підтримці міжнародної співпраці у сфері кібербезпеки. Корейські закони, такі як Закон про захист інформації, забезпечують високий рівень захисту персональних даних та конфіденційності, що дозволяє користувачам мати більше контролю над своєю інформацією. Південна Корея активно співпрацює з міжнародними організаціями та іншими країнами, що робить її одним із лідерів у розвитку механізмів протидії кіберзлочинності в глобальному масштабі. Цей підхід сприяє не лише захисту особистих даних, а й створенню середовища для інновацій та розвитку цифрової економіки [23, с.19].

Таким чином, підходи до законодавства у сфері кіберзлочинності в Китаї та Південній Кореї ілюструють різні погляди на баланс між безпекою та правами користувачів. Китайський контроль за інформацією забезпечує надійний захист від загроз, але за рахунок прав і свобод громадян, тоді як Південна Корея намагається знайти компроміс між захистом даних та підтримкою інновацій. Ці різні підходи демонструють, як важливо враховувати національні контексти при розробці ефективних стратегій у боротьбі з кіберзлочинністю.

В Україні було здійснено значні кроки у регулюванні кібербезпеки, що свідчить про усвідомлення важливості цього питання в сучасному світі. Прийнятий у 2017 році Закон України «Про основні засади забезпечення кібербезпеки» став важливим кроком у формуванні правових та організаційних основ для кіберзахисту держави. Цей закон визначає основні принципи та механізми забезпечення кібербезпеки, а також закладає фундамент для співпраці між державними органами, приватним сектором та громадськістю в питаннях кіберзахисту.

У рамках реалізації цього закону було створено низку національних структур, які відповідають за кіберзахист критичної інфраструктури. Однією з таких структур є Державна служба спеціального зв’язку та захисту інформації України. Цей орган виконує функції з моніторингу та захисту інформаційних

систем, реагування на кіберінциденти та забезпечення надійності роботи критичної інфраструктури. Завдяки своїй діяльності, Державна служба стала ключовим елементом у протидії кіберзагрозам, надаючи експертну підтримку, а також здійснюючи аналіз і оцінку ризиків у сфері кібербезпеки.

Крім того, в Україні активно розвиваються програми підготовки фахівців у галузі кібербезпеки, що є важливим аспектом для забезпечення ефективного захисту від кіберзлочинності. Зростаюча увага до кібербезпеки з боку держави, а також співпраця з міжнародними організаціями, сприяють створенню ефективної системи захисту в умовах зростаючих кіберзагроз. Цей процес потребує не лише вдосконалення законодавства, але й інвестицій у технології та підготовку кадрів, що дозволить Україні стати більш стійкою до кіберзлочинності та підвищить загальний рівень безпеки інформаційного середовища.

Кіберзлочинність, яка здійснюється через державні кордони та вражає громадян і економіку різних країн, потребує спільних зусиль для її ефективного подолання. Зважаючи на різні підходи до кібербезпеки та регулювання кіберзлочинності, держави мають потребу в узгодженні своїх законодавств і взаємному визнанні правових норм. Без цього міжнародна співпраця в галузі кібербезпеки значно ускладнена, адже деякі країни можуть використовувати різницю в законах для уникнення відповідальності або навіть як тактику у конфліктах.

Сучасні технологічні досягнення, як-от блокчейн, криптовалюти та штучний інтелект, створюють нові ризики та виклики для регулювання кіберзлочинності. Наприклад, анонімність криптовалют дозволяє злочинцям приховувати свою діяльність, що ускладнює правоохоронним органам відстеження незаконних транзакцій. Штучний інтелект, зокрема, може використовуватися як для посилення захисту, так і для автоматизації кіберзлочинів, включно з фішинговими атаками та розсилкою шкідливого програмного забезпечення.

Крім того, кіберзлочинність ускладнюється новими формами атак, як-от атаки типу «відмова в обслуговуванні» (DDoS), кібершпигунство та поширення шкідливих програм. Такі атаки часто здійснюються з метою підриву економічної та політичної стабільності, а також для доступу до конфіденційної інформації.

Відтак, кіберзлочинність є мультидисциплінарною проблемою, що вимагає інтеграції правових, технічних та організаційних підходів на міжнародному та національному рівнях. Розвиток глобальної кібербезпеки потребує як модернізації міжнародного права, так і активної співпраці між країнами. Лише шляхом об’єднання зусиль можна ефективно боротися з кіберзлочинністю, яка загрожує глобальній стабільності та безпеці.

РОЗДІЛ 2.
ВИКЛИКИ КІБЕРБЕЗПЕКИ ДЛЯ ПРАВООХОРОННИХ ОРГАНІВ

2.1. Сучасні загрози кібербезпеці та їх вплив на діяльність правоохоронних органів

Сучасні загрози кібербезпеці мають серйозний вплив на правоохоронні органи, оскільки з кожним роком кіберпростір стає важливішою частиною життя суспільства, а отже, зростає і його вразливість до атак. У цифровій епосі кіберзлочинці, терористичні угруповання та державні хакери використовують новітні методи, щоб зламати захисні системи, обійти традиційні заходи безпеки та поставити під загрозу функціонування як окремих структур, так і цілих держав. Такі атаки можуть призводити до збоїв у системах державного управління, що своєю чергою негативно впливає на суспільну безпеку та стабільність.

Однією з найбільших загроз для правоохоронних органів сьогодні є цільові кібератаки, метою яких є отримання контролю над критичною інфраструктурою або базами даних, що містять надзвичайно важливу інформацію. Кіберзлочинці фокусуються на системах, де зберігаються стратегічні дані, такі як відомості про розслідування, особисті дані свідків, оперативні методи роботи та інша конфіденційна інформація. Витік цих даних може призвести до катастрофічних наслідків, починаючи від порушення процесів розслідування та до загрози життю співробітників правоохоронних органів [24, с.165].

Контроль над критичною інфраструктурою, якою користуються правоохоронні органи, дозволяє зловмисникам впливати на загальну систему безпеки держави. Атаки такого типу можуть паралізувати діяльність правоохоронних органів і значно ускладнити виконання їхніх функцій. Крім того, доступ до стратегічної інформації може спровокувати викриття та

ідентифікацію агентів або оперативників, що безпосередньо ставить під загрозу їхню особисту безпеку та ефективність роботи.

Важливим аспектом цієї загрози є те, що наслідки витоку інформації можуть поширюватися на широке коло осіб, залучених до розслідувань, і надавати зловмисникам можливість впливати на хід правосуддя. Наприклад, доступ до даних про свідків або жертв злочинів дозволяє залякувати їх або вживати заходи, щоб уникнути правової відповідальності. У такому контексті особливо актуальною є розробка новітніх механізмів захисту даних та підвищення рівня кібербезпеки, аби мінімізувати можливі ризики від цільових атак [24, с.167].

Кіберзлочинність розвивається надзвичайно швидкими темпами, часто випереджаючи зусилля правоохоронців щодо адаптації до нових умов. Одним із найяскравіших проявів цієї динаміки є використання кіберзлочинцями шкідливого програмного забезпечення, спеціально розробленого для обходу звичних механізмів захисту. Сучасні кіберзлочинці застосовують цілий арсенал технологій, що дозволяють проникати у захищені системи, уникати виявлення та завдавати цілеспрямованих ударів по критичній інфраструктурі. Вразливість правоохоронних органів у такій ситуації є особливо критичною, оскільки будь-який збій у роботі може мати серйозні наслідки для безпеки суспільства [25, с.600].

Одним з найбільш поширених інструментів, які використовуються для атак, є програми типу «Ransomware» або програми-вимагачі. Їхня тактика полягає в блокуванні доступу до інформації або систем, з вимогою викупу для відновлення доступу. Коли такі програми вражають системи правоохоронних органів, це може призвести до тимчасової втрати доступу до критично важливих даних, зупинки оперативних процесів і паралічу ключових функцій. Для правоохоронців це означає, що в певний момент вони можуть втратити доступ до баз даних, у яких зберігаються докази, важливі відомості про свідків, підозрюваних або навіть записи про хід розслідувань.

Оскільки вимагання зазвичай супроводжується погрозами остаточного знищення даних у разі невиплати викупу, правоохоронні органи опиняються перед складним вибором: ризикувати безпекою важливих відомостей або вести переговори з кіберзлочинцями, що створює небезпечний прецедент і підриває довіру суспільства до здатності правоохоронців захищати не тільки себе, а й громадян. Тому для правоохоронців важливо мати ефективні протоколи реагування на такі атаки та швидко вдосконалювати кіберзахист, аби знизити вразливість перед подібними загрозами.

Фінансові установи, державні органи та правоохоронні структури сьогодні перебувають під постійною загрозою кібератак, які орієнтовані на доступ до фінансових ресурсів або конфіденційної інформації. Ці інциденти не тільки спричиняють значні фінансові втрати, але й створюють серйозну загрозу для економічної стабільності країни, оскільки зловмисники можуть маніпулювати великими обсягами ресурсів або паралізувати діяльність стратегічно важливих структур. Порушення безпеки та потенційні витоки чутливих даних суттєво підривають довіру громадян до здатності державних органів забезпечувати належний захист інформації та надавати ефективні послуги [25, с.602].

На додачу, зловмисники активно вдосконалюють свої методи соціальної інженерії, використовуючи психологічний вплив для маніпуляції користувачами та введення їх в оману. Вони змушують людей, часто несвідомо, надавати доступ до конфіденційної інформації або виконувати дії, які відкривають двері до системи. Соціальна інженерія стала потужним інструментом, який дозволяє зловмисникам не лише обійти технічні засоби безпеки, але й залучати працівників самих установ до власних схем, роблячи їх свого роду «агентами», що ускладнює виявлення злочинців і попередження атак.

Для правоохоронців це означає потребу в постійному вдосконаленні методів протидії кіберзлочинам. Стандартні методи безпеки тепер повинні доповнюватися більш комплексними підходами, що включають

просвітницьку роботу серед співробітників та громадян, а також створення ефективних інструментів виявлення психологічного впливу зловмисників. В умовах, коли навіть досвідчені працівники можуть стати жертвами соціальної інженерії, завдання правоохоронців стає надзвичайно складним і потребує нових рішень та стратегії для збереження стабільності та захисту державних ресурсів [26, с.79].

Технології штучного інтелекту створюють нові виклики у сфері кібербезпеки, оскільки зловмисники швидко адаптуються до нових можливостей і застосовують ШІ для автоматизації та масштабування своїх атак. Завдяки цьому їм вдається оптимізувати процеси створення та поширення шкідливого програмного забезпечення, а також зробити їхні дії менш передбачуваними для систем захисту. ШІ надає зловмисникам змогу створювати адаптивні шкідливі програми, які змінюють свою поведінку в реальному часі, аби уникати детекції навіть при наявності найсучасніших методів захисту. Такі технології не лише збільшують складність атак, а й знижують ефективність існуючих засобів захисту, оскільки традиційні методи ідентифікації загроз не завжди можуть впоратися з динамічною природою адаптивного шкідливого ПЗ.

Для правоохоронних органів це стає серйозною проблемою, оскільки впровадження інновацій для захисту від таких загроз вимагає значних ресурсів і постійного оновлення технологій. У контексті використання ШІ кіберзлочинцями правоохоронцям доводиться не тільки покращувати наявні методи ідентифікації шкідливого ПЗ, але й працювати над створенням власних систем штучного інтелекту, які здатні оперативно виявляти нові види загроз та аналізувати їх у реальному часі. Це потребує інвестицій у дослідження, підготовку кадрів та інтеграцію передових рішень, які можуть протистояти змінним і дедалі більш комплексним атакам [26, с.80].

З кожною новою атакою, що використовує штучний інтелект, кібербезпекові методи, які вважалися надійними, втрачають свою актуальність. Правоохоронні органи змушені вдосконалюватися, не тільки

щоб ефективно реагувати на конкретні загрози, але й щоб передбачати їх розвиток, що можливо лише через впровадження глибокої аналітики та машинного навчання. В умовах, коли зловмисники швидко вчаться обходити традиційні бар’єри безпеки, правоохоронцям необхідно створювати комплексні системи, що зможуть адаптуватися та випереджати кіберзагрози, забезпечуючи довготривалий захист даних і функціональності критичних систем.

Правоохоронні органи сьогодні стикаються з новими викликами, пов'язаними з розвитком технології «Інтернету речей» (IoT). Це явище суттєво змінює ландшафт безпеки, оскільки надає зловмисникам нові можливості для отримання доступу до фізичних пристроїв, які підключені до мережі. Від камери відеоспостереження та систем контролю доступу до автомобілів — кожен з цих елементів може стати мішенню для хакерів. Вони можуть отримувати контроль над цими пристроями, маніпулюючи ними для своїх цілей, що безпосередньо загрожує фізичній безпеці правоохоронців і громадян [27, с.45].

Наприклад, якщо зловмисник отримає доступ до системи відеоспостереження, він може спостерігати за рухами правоохоронців, виявляти їх стратегії та розробки, а також планувати свої дії з урахуванням інформації, отриманої через такі системи. Це може призвести до серйозних наслідків, таких як підрив безпеки проведення оперативних заходів або навіть загроза життю співробітників поліції, якщо хакери зможуть з'ясувати деталі їхньої роботи. З огляду на це, важливо, щоб правоохоронні органи адаптували свої стратегії безпеки, враховуючи нові технології та вразливості, що виникають внаслідок їхнього впровадження.

Крім того, потенційні загрози, пов'язані з IoT, зобов'язують правоохоронців активно працювати над розробкою нових протоколів безпеки та інвестиціями в технології, які можуть запобігти таким атакам. Це включає в себе моніторинг підключених пристроїв, їхнє постійне оновлення та впровадження складних систем аутентифікації. Аби ефективно боротися з

кіберзагрозами, правоохоронні органи повинні зрозуміти, що IoT — це не лише нові можливості, але й нові виклики, які потребують комплексного підходу та готовності до адаптації у швидко змінюваному цифровому середовищі [28, с.5].

У зв'язку з постійними викликами в галузі кібербезпеки держави змушені невпинно оновлювати законодавство та стандарти для ефективного протистояння кіберзлочинцям. Однак законодавчі ініціативи часто не встигають за технологічними змінами, що створює юридичні «прогалини», якими охоче користуються зловмисники. Ці прогалини можуть бути використані для уникнення покарання або навіть для легалізації деяких дій, які насправді є злочинними, але не підпадають під дію чинного законодавства. Крім того, міжнародний характер кіберзлочинів ускладнює процес розслідування та покарання, адже правові системи різних країн можуть суттєво відрізнятися, що ускладнює співпрацю та взаємодію між державами.

Однією з важливих складових ефективної боротьби з кіберзлочинністю є навчання правоохоронців новим технологіям та методам реагування на кіберзагрози. У сучасних умовах, коли загрози постійно еволюціонують, важливо, щоб співробітники мали можливість швидко розпізнавати нові форми атак та адаптувати свої методи розслідування. Навчальні програми, орієнтовані на кібербезпеку, дозволяють правоохоронцям краще розуміти методи, які використовують зловмисники, а також забезпечують необхідні навички для оперативного реагування на кібератаки [29, с.81].

Таке навчання включає в себе різноманітні аспекти, від вивчення основ кібербезпеки та нових технологій до розробки сценаріїв реагування на конкретні ситуації. Залучення фахівців у сфері кібербезпеки до підготовки правоохоронців також може стати важливим кроком до покращення їхньої готовності до протидії кіберзагрозам. У підсумку, систематичне навчання і вдосконалення навичок співробітників стає ключовим елементом у боротьбі з кіберзлочинністю, адже воно дозволяє правоохоронним органам швидше

реагувати на нові виклики та зберігати контроль над ситуацією в умовах постійно змінюваного цифрового середовища.

Попри всі зусилля правоохоронних органів, кіберзлочинці вдосконалюють методи шифрування та анонімізації, що ускладнює їх ідентифікацію. Відомі сервіси типу Darknet надають злочинцям платформи для обміну інформацією, торгівлі зброєю, наркотиками та навіть організації терористичних атак. Протидія таким злочинам вимагає від правоохоронних органів як технологічної, так і інформаційної підготовки для швидкого виявлення злочинців і ліквідації загроз.

Загрози кібербезпеці можуть також мати серйозні соціальні наслідки. Кібератаки на державні установи чи комунальні послуги можуть призводити до порушення роботи критично важливих систем, таких як енергетика, водопостачання чи транспорт. Це може спричинити паніку серед населення, загрозу безпеці життя та здоров'я громадян, а також підривати довіру до органів державної влади та правоохоронців.

Кіберзагрози змінюють традиційні методи розслідувань, тому правоохоронним органам доводиться використовувати нові підходи та технології, такі як кіберрозвідка, аналіз великих даних та штучний інтелект для відстеження та передбачення дій злочинців. Це дозволяє виявляти потенційні загрози ще до їхнього виникнення, проте вимагає значних фінансових ресурсів та спеціалізованої підготовки [29, с.82].

У сучасному кіберпросторі співробітництво між правоохоронними органами різних країн стає дедалі більш важливим і необхідним у боротьбі з кіберзлочинністю. Завдяки глобальному характеру кіберзагроз, які не знають кордонів, країни повинні об'єднувати свої зусилля для ефективного протистояння цим викликам. Міжнародні організації, такі як Інтерпол та Європол, активно розвивають спільні ініціативи, створюючи центри з боротьби з кіберзлочинністю, де здійснюється обмін інформацією про нові загрози, методи роботи злочинців та технології для їх виявлення та нейтралізації.

Таке співробітництво дозволяє країнам не тільки швидше реагувати на кіберінциденти, але й створювати більш комплексні стратегії для боротьби з глобальними кіберзлочинами. Завдяки обміну інформацією, правоохоронні органи можуть отримувати дані про тенденції та моделі поведінки кіберзлочинців, що допомагає їм розробляти проактивні заходи та вдосконалювати власні системи безпеки. Спільні тренінги та навчальні програми також сприяють підвищенню кваліфікації співробітників, дозволяючи їм краще розуміти специфіку кіберзлочинності в різних регіонах.

Крім того, такі центри створюють платформу для міжнародного співробітництва, де правоохоронці можуть ділитися досвідом та обговорювати найкращі практики у протидії кіберзагрозам. Це взаємодоповнює зусилля країн у створенні законодавчої бази, що враховує особливості кіберзлочинності, і забезпечує більшу ефективність у проведенні розслідувань на міжнародному рівні. У підсумку, розвиток співробітництва між країнами у сфері боротьби з кіберзлочинністю не тільки підвищує рівень безпеки, а й зміцнює міжнародні зв’язки, сприяючи більшій стабільності у глобальному кіберпросторі [30, с.299].

Отже, сучасні загрози кібербезпеці мають значний вплив на діяльність правоохоронних органів. Вони вимагають від них нових підходів до організації роботи, постійної адаптації до нових технологічних змін, а також активного міжнародного співробітництва. Лише через ефективну взаємодію, впровадження новітніх технологій та постійне підвищення кваліфікації співробітників можна досягти успішної протидії цим викликам.

2.2. Методи та засоби захисту від кіберзлочинності: міжнародний досвід і практика в Україні

Озброєна потужними технологіями, кіберзлочинність стає глобальною загрозою для держав, бізнесу та громадян. Кількість і складність кіберзлочинів неухильно зростають, що змушує уряди всього світу переглядати свої підходи

до кібербезпеки. Однією з основних складових боротьби з кіберзлочинністю є розробка й упровадження ефективних методів та засобів захисту. Важливо розглядати не лише технічні аспекти, а й стратегічні, організаційні й правові методи боротьби, які активно застосовують у різних країнах і можуть стати корисним досвідом для України.

Сучасна кібербезпека зосереджується на трьох основних аспектах: виявленні загроз, запобіганні кіберінцидентам та оперативному реагуванні на них. Одним із ключових інструментів у цій боротьбі є моніторинг мережевого трафіку, який дозволяє виявляти підозрілі активності на ранніх стадіях, таким чином забезпечуючи можливість вжити необхідні заходи до того, як кіберінцидент призведе до серйозних наслідків. Технології моніторингу стають все більш складними, проте їхня ефективність значно підвищується, коли вони використовуються в поєднанні з іншими засобами безпеки [31, с.127].

Для забезпечення багаторівневого захисту інформаційних систем необхідно інтегрувати моніторинг з антивірусним програмним забезпеченням, системами виявлення та запобігання вторгненням (IDS/IPS), а також інструментами криптографічного захисту даних. Це комплексне рішення дозволяє створити більш надійну систему захисту, яка не лише виявляє загрози, а й активно блокує їх до того, як вони зможуть завдати шкоди. Важливим компонентом такої системи є контроль доступу до даних, який допомагає обмежити можливості кіберзлочинців, зменшуючи ризик витоку чутливої інформації.

Контроль доступу дозволяє організаціям визначати, хто має право на доступ до певних даних і ресурсів, обмежуючи привілеї користувачів відповідно до їхніх посадових обов'язків. Це особливо важливо в умовах, коли внутрішні загрози можуть бути не менш небезпечними, ніж зовнішні. Ретельний підбір рівнів доступу і регулярні перевірки користувачів допомагають запобігти несанкціонованому доступу, що, в свою чергу, знижує ризики, пов'язані з витоками інформації та іншими кіберзлочинами [31, с.130].

Навчання персоналу та інформування громадян про кіберризики є одним із найбільш ефективних методів запобігання кіберінцидентам. Міжнародний досвід показує, що значну частину таких інцидентів можна уникнути, якщо співробітники компаній та організацій мають необхідні знання щодо фішингових атак, методів соціальної інженерії та правил безпечного використання інтернету. Розуміння цих загроз і вміння їх ідентифікувати дозволяє знизити ймовірність успішних атак.

Прикладом системного підходу до кіберосвіти є ініціативи Європейського Союзу, які активно впроваджують програми підвищення обізнаності серед населення. Ці програми включають в себе тренінги для співробітників компаній та державних установ, які допомагають їм розуміти актуальні загрози та ефективно реагувати на них. Важливо, що ці заходи не обмежуються лише навчанням працівників, але й включають інформаційні кампанії для широких верств населення.

Такі кампанії можуть містити різноманітні формати: вебінари, інформаційні буклети, відеоролики та соціальні медіа-акції, спрямовані на роз'яснення важливості безпеки в інтернеті. Залучення громадян до навчання про кібербезпеку сприяє формуванню культури безпечного користування цифровими технологіями, що в свою чергу зменшує ризик кіберзлочинності [32, с.128].

Крім того, організації можуть створювати внутрішні програми навчання, які забезпечують регулярне оновлення знань співробітників. Це важливо в умовах швидкого розвитку технологій та методів атак. Завдяки постійному навчанню та підвищенню обізнаності про кіберризики, організації можуть суттєво зменшити ймовірність успіху кіберзлочинців та підвищити загальний рівень безпеки у своїй діяльності. У результаті, інвестиції в освіту та підготовку стають необхідними для створення стійкого середовища, яке здатне ефективно протистояти сучасним кіберзагрозам.

Створення спеціалізованих кіберпідрозділів у правоохоронних органах є ще одним ефективним засобом протидії кіберзлочинності. Ці підрозділи

надають можливість зосередити експертизу, ресурси та технології на боротьбі з кіберзлочинами, що вимагають особливого підходу та знань. Наприклад, Європол має свій Центр боротьби з кіберзлочинністю (ЕС3), який виконує важливу роль у координації розслідувань кіберзлочинів, обміні інформацією між країнами та впровадженні спільних операцій. Подібні підрозділи функціонують у таких країнах, як США, Велика Британія та Німеччина, демонструючи успішність цього підходу.

Для України важливо розвивати потужні кіберпідрозділи, що забезпечать ефективне запобігання та реагування на кіберзлочинність. Хоча в Україні вже існують такі підрозділи, їхня ефективність може бути значно підвищена через додаткові інвестиції та міжнародну співпрацю. Залучення іноземних експертів та передових технологій у галузі кібербезпеки дозволить українським правоохоронцям отримати нові знання та навички, а також впроваджувати сучасні методи розслідування [33, с.183].

Крім того, важливо забезпечити належну матеріально-технічну базу для таких підрозділів. Це може включати в себе не лише програмне забезпечення, але й апаратні рішення, навчання персоналу та участь у міжнародних тренінгах та конференціях. Співпраця з іншими країнами, обмін інформацією про кіберзагрози та досвід у розслідуваннях можуть стати вирішальними факторами для успіху в цій сфері.

У результаті, інвестиції в розвиток кіберпідрозділів та їх інтеграція у міжнародні мережі співпраці можуть суттєво підвищити рівень захисту України від кіберзлочинності. Це стане важливим кроком до створення надійної системи кібербезпеки, здатної ефективно протистояти сучасним викликам у цифровому середовищі [33, с.185].

Розробка законодавчих ініціатив, що відповідають сучасним викликам кіберзлочинності, є одним з найкритичніших аспектів у боротьбі з цією загрозою. На міжнародному рівні значним досягненням стало прийняття Будапештської конвенції про кіберзлочинність, яка є першим міжнародним договором, що визначає основні підходи до боротьби з кіберзлочинністю. Ця

конвенція забезпечує правову основу для співпраці між державами, що в свою чергу дозволяє створювати більш ефективні механізми реагування на кіберзлочини.

Приєднання України до Будапештської конвенції стало важливим кроком до інтеграції міжнародних стандартів у вітчизняне законодавство. Це відкриває можливості для адаптації українських законів до світових практик, що допоможе краще реагувати на нові загрози у сфері кібербезпеки. Проте законодавче забезпечення повинно бути динамічним і постійно оновлюватись, адже методи, які використовують кіберзлочинці, змінюються швидко. Тому важливо забезпечити гнучкість законодавства, яке може оперативно реагувати на нові виклики, що виникають у кіберпросторі [33, с.186].

Будапештська конвенція також акцентує увагу на важливості активної міжнародної співпраці. Це дозволяє країнам-учасницям обмінюватись оперативною інформацією про кіберзагрози, методи атак та шляхи їхнього попередження. Спільна робота над розслідуваннями та обмін досвідом у боротьбі з транснаціональною кіберзлочинністю є необхідними для забезпечення ефективності правоохоронних органів.

У сучасному світі багато країн активно впроваджують штучний інтелект (ШІ) та машинне навчання як інструменти для покращення кіберзахисту. Ці технології дозволяють виявляти аномалії в поведінці користувачів, аналізувати великі обсяги даних і прогнозувати можливі кібернапади. ШІ має потенціал автоматизувати процеси кіберзахисту, що значно підвищує ефективність виявлення загроз і знижує ризики для організацій.

Наприклад, у США активно розробляють системи, засновані на машинному навчанні, які здатні аналізувати моделі поведінки користувачів. Ці системи можуть виявляти потенційні загрози ще до того, як вони стануть помітними на рівні мережевого трафіку. Завдяки цьому кіберзахисники отримують можливість реагувати на загрози на ранніх стадіях, що суттєво зменшує можливість успішних атак [34, с.59].

Для України доцільно переймати цей досвід, впроваджуючи технології штучного інтелекту у сферах, де потрібна швидка обробка великих обсягів інформації. Використання ШІ може стати ключовим фактором у модернізації системи кібербезпеки країни, адже в умовах постійно змінюваних загроз важливо мати інструменти, які здатні швидко адаптуватися до нових викликів.

Інтеграція ШІ у правоохоронні органи та інші державні установи також може підвищити їхню спроможність до аналізу даних і прийняття рішень на основі отриманої інформації. Це дозволить не лише ефективно реагувати на кіберзагрози, але й прогнозувати їх розвиток, що стане важливим елементом стратегії забезпечення національної безпеки.

В цілому, використання штучного інтелекту та машинного навчання у сфері кібербезпеки є перспективним напрямком, який може суттєво підвищити рівень захисту інформаційних систем і зменшити ризики, пов'язані з кіберзлочинністю.

Для ефективної боротьби з кіберзлочинністю встановлення тісних зв'язків між державними установами, бізнесом і науковими організаціями є вкрай важливим. Цей підхід довів свою дієвість у США, де реалізуються програми державно-приватного партнерства, що об'єднують зусилля уряду, приватного сектора і наукової спільноти для покращення загальної кібербезпеки. Завдяки такій колаборації можливо обмінюватись інформацією про загрози, розвивати спільні технології та практики захисту, а також організовувати навчальні програми для підвищення кваліфікації фахівців [34, с.61].

В Україні важливо налагодити аналогічні партнерства між правоохоронними органами та комерційними організаціями. Таке співробітництво дозволить швидше реагувати на кіберінциденти, оскільки комерційні структури часто мають доступ до передових технологій та досвіду, що може бути корисним для державних установ. Наприклад, спільна робота над проектами в сфері кібербезпеки може призвести до розробки нових рішень для виявлення та нейтралізації кіберзагроз.

Крім того, бізнес може бути зацікавлений у підвищенні загального рівня захищеності приватного сектору, оскільки це безпосередньо впливає на їхню діяльність і репутацію. Впровадження спільних ініціатив може включати проведення навчальних семінарів, спільних навчань з реагування на кіберінциденти та обмін даними про виявлені загрози. Це дозволить не лише зменшити ризики, пов'язані з кіберзлочинністю, але й створити ефективну модель взаємодії, яка зможе адаптуватись до нових викликів у цифровому середовищі [35, с.92].

Ключовим викликом для України залишається інтеграція сучасних технологій і підходів до боротьби з кіберзлочинністю в національну стратегію кібербезпеки. В умовах постійно змінюваного кіберпростору та розвитку нових загроз система кібербезпеки країни потребує комплексної модернізації, що враховує як міжнародний досвід, так і специфіку загроз, з якими стикається Україна.

Модернізація системи кібербезпеки повинна включати не лише впровадження передових технологій, таких як штучний інтелект, машинне навчання та інструменти для автоматизації кіберзахисту, але й акцент на підвищення кваліфікації фахівців у цій сфері. Це передбачає розробку та реалізацію навчальних програм, які б охоплювали новітні тенденції в кібербезпеці та забезпечували б спеціалістів знаннями та навичками, необхідними для успішної боротьби з кіберзлочинністю.

Крім того, важливим аспектом є розвиток аналітичних центрів та дослідницьких лабораторій, які спеціалізуються на питаннях кібербезпеки. Такі установи можуть виступати платформою для обміну знаннями та досвідом, сприяючи розробці нових методів і технологій для виявлення та нейтралізації кіберзагроз. Вони також можуть слугувати майданчиком для співпраці між державними структурами, бізнесом та академічними установами, що дозволить створити цілісну екосистему кібербезпеки [36, с.49].

Приділяючи увагу підготовці кадрів та розвитку наукових досліджень, Україна зможе забезпечити собі конкурентну перевагу у сфері кібербезпеки. Це не лише підвищить ефективність боротьби з кіберзлочинністю, але й сприятиме загальному розвитку інформаційних технологій у країні, що, в свою чергу, позитивно позначиться на економіці та соціальному добробуті громадян.

Важливою частиною національної стратегії кібербезпеки має стати співпраця з міжнародними організаціями. Активна участь України в програмах Європейського Союзу, НАТО та ООН вже свідчить про її прагнення до інтеграції в глобальні безпекові структури та підвищення власних стандартів у сфері кіберзахисту. Проте для досягнення більш значущих результатів необхідно поглибити такі ініціативи та активно долучатися до міжнародних проектів.

Співпраця з міжнародними організаціями дозволяє Україні отримати доступ до найновіших технологій і методик у сфері кібербезпеки, що є вирішальним фактором у боротьбі з кіберзлочинністю. Цей доступ включає в себе обмін інформацією про нові загрози, найкращі практики реагування на кіберінциденти та можливості спільного навчання. Крім того, міжнародні проекти можуть надавати Україні підтримку у формуванні національних стандартів кібербезпеки, що базуються на міжнародних нормах [36, с.51].

Крім того, тісна співпраця з міжнародними партнерами може спростити інтеграцію в глобальні системи реагування на кіберзагрози, що особливо важливо в умовах транснаціональної природи сучасної кіберзлочинності. Спільні тренінги та навчальні програми, реалізовані у рамках міжнародних ініціатив, допоможуть українським фахівцям підвищити рівень підготовки та готовності до реагування на нові виклики.

Фінансування й інвестиції в дослідження кібербезпеки є ще одним важливим елементом успішної боротьби з кіберзлочинністю. Міжнародний досвід показує, що країни, які вкладають кошти в дослідження й розробку технологій кібербезпеки, мають значну перевагу. Наприклад, США й Велика

Британія активно підтримують наукові установи, які працюють у галузі кібербезпеки, що дозволяє цим країнам підтримувати високий рівень технологічної підготовленості. Україні слід звернути увагу на необхідність фінансової підтримки кібербезпекових ініціатив, що дозволить стимулювати розвиток цієї сфери й залучити нові кадри.

Кіберзахист стає важливим аспектом національної безпеки України, що вимагає не тільки використання технічних засобів захисту, а й розвитку правового й організаційного середовища. Впровадження міжнародного досвіду в галузі кібербезпеки може стати ефективним інструментом для зменшення рівня кіберзлочинності й підвищення загальної стійкості країни до кіберзагроз.

2.3. Використання новітніх технологій у протидії кіберзлочинності: перспективи та проблеми

Кіберзлочинність в Україні, як і в усьому світі, швидко зростає. Еволюція загроз у кіберпросторі, розповсюдження складних шкідливих програм, соціальна інженерія та атаки на критичну інфраструктуру спонукають до розробки новітніх засобів захисту. Україна, як держава з розвиненими IT-ресурсами, стикається з особливими викликами: її кіберпростір часто стає мішенню як зовнішніх, так і внутрішніх атак, що вимагає застосування новітніх технологій для протидії кіберзлочинності.

На початку варто зазначити, що розвиток сучасних технологій дає правоохоронним органам низку інструментів для виявлення та запобігання кіберзагрозам. Штучний інтелект (ШІ) та машинне навчання стають одними з основних засобів аналізу кіберзагроз. Алгоритми ШІ дозволяють автоматично обробляти великі обсяги даних, виявляти підозрілі моделі поведінки, відслідковувати кіберзагрози в режимі реального часу та прогнозувати нові форми атак. Це має особливе значення для українських правоохоронних

органів, оскільки швидкість виявлення та реагування на кіберзагрози безпосередньо впливає на рівень національної безпеки [37, с.152].

Іншим перспективним напрямом у сфері кібербезпеки є застосування технологій аналізу великих даних (Big Data). Ці технології, разом із хмарними рішеннями, відкривають нові можливості для аналізу інформації з різних джерел, включно з соціальними мережами, платформами обміну файлами та іншими відкритими ресурсами. Збираючи та аналізуючи ці великі обсяги даних, правоохоронні органи можуть виявляти закономірності та тенденції у поведінці кіберзлочинців, що значно підвищує ефективність запобігання злочинам ще до їх здійснення.

Аналіз великих даних дозволяє виявляти підозрілі патерни поведінки, які можуть свідчити про підготовку до кіберзлочину. Наприклад, виявлення аномальної активності у мережах або в соціальних медіа може служити сигналом для правоохоронців про можливі загрози. Це, у свою чергу, дає змогу оперативно реагувати на потенційні атаки, що знижує ризики для критичної інфраструктури та забезпечує безпеку громадян [37, с.190].

Хоча в Україні цей напрямок наразі перебуває на початковому етапі розвитку, його потенціал для виявлення загроз в режимі реального часу є значним. Використання великих даних може суттєво поліпшити ситуацію з кібербезпекою в країні, надаючи можливості для більш швидкого та точного реагування на загрози. Інтеграція технологій Big Data в структури правоохоронних органів, а також підготовка фахівців у цій сфері стануть важливими кроками для підвищення ефективності боротьби з кіберзлочинністю.

Блокчейн-технологія стає все більш важливою у боротьбі з фінансовою кіберзлочинністю завдяки своїм унікальним характеристикам, які забезпечують прозорість і надійність зберігання даних. Основною перевагою блокчейну є його здатність вести незмінний реєстр всіх транзакцій, що дозволяє легко відстежувати рух коштів. Ця технологія застосовується для моніторингу фінансових операцій, виявлення аномалій та незаконних потоків,

що особливо актуально в умовах зростаючої популярності криптовалют. Блокчейн не лише забезпечує прозорість, а й дозволяє забезпечити захист від маніпуляцій, оскільки зміни в записах потребують консенсусу всіх учасників мережі.

У контексті України, де використання криптовалют все частіше стає частиною злочинних схем, застосування блокчейну виглядає надзвичайно актуальним. Відзначаючи високий рівень злочинності, пов’язаної з фінансовими транзакціями, українські правоохоронні органи все більше зацікавлені у використанні блокчейн-технології для виявлення і розслідування кіберзлочинів. Це не лише допомагає виявляти незаконні фінансові потоки, але й служить основою для збору доказів, які можуть бути використані в судовому розгляді. Застосування блокчейну у цій сфері підкреслює необхідність інтеграції новітніх технологій у стратегії кібербезпеки [38, с.165].

Зростаюча довіра до блокчейн-технології свідчить про її потенціал у забезпеченні більш безпечного середовища для фінансових операцій. Блокчейн може стати важливим інструментом у зусиллях держави щодо підвищення прозорості економічних відносин, зменшення ризиків фінансової злочинності та покращення загальної ситуації з кібербезпекою в країні. Ефективне використання цієї технології може значно знизити ризики, пов'язані з шахрайством і відмиванням грошей, а також підвищити рівень захисту для законних користувачів фінансових систем. Таким чином, блокчейн не лише зміцнює фінансову безпеку, а й сприяє формуванню довіри до цифрових фінансових інститутів.

Багатофакторна автентифікація та біометричні системи стають одними з найбільш значущих інструментів у боротьбі з кіберзлочинністю, завдяки своїй здатності підвищувати рівень безпеки в обробці та зберіганні даних. Використання біометричних характеристик, таких як відбитки пальців, розпізнавання обличчя і голосу, дозволяє створити надійні механізми ідентифікації користувачів. Ці технології не лише ускладнюють процес несанкціонованого доступу, але й створюють надійну основу для захисту

особистої та корпоративної інформації. Особливо це важливо в сучасному світі, де загрози кіберзлочинності постійно зростають [38, с.166].

В Україні банки та фінансові установи активно впроваджують біометричні дані для забезпечення безпеки своїх клієнтів. Цей крок став відповіддю на зростаючі ризики, пов'язані з крадіжкою особистих даних і фінансовими шахрайствами. Наприклад, технології розпізнавання обличчя дозволяють користувачам безпечно входити в онлайн-банкінг, у той час як голосові біометричні системи можуть служити надійним засобом підтвердження особи при телефонних запитах до служби підтримки. Це підвищує рівень довіри з боку клієнтів і забезпечує вищий рівень захисту для фінансових транзакцій [39, с.43].

Хоча впровадження таких технологій вимагає значних інвестицій і зусиль, їхня ефективність у запобіганні кіберзлочинам є очевидною. Інвестиції в розвиток систем біометричної автентифікації можуть виправдати себе, оскільки зменшують ймовірність витоку даних і фінансових збитків. Додатково, такі системи можуть знижувати навантаження на служби підтримки, оскільки зменшують кількість випадків, коли клієнти забувають свої паролі або не можуть підтвердити свою особистість. Таким чином, багатофакторна автентифікація та біометричні системи не тільки підвищують загальний рівень безпеки, але й роблять процеси управління даними більш зручними для користувачів.

Незважаючи на значні можливості, які новітні технології надають у боротьбі з кіберзлочинністю, вони також породжують нові виклики, зокрема в контексті конфіденційності та захисту особистих даних. Наприклад, використання технологій штучного інтелекту та аналізу великих даних для моніторингу активності користувачів передбачає збір і обробку величезних обсягів персональної інформації. Це, у свою чергу, піднімає питання прав людини на приватність, оскільки без належного контролю та регулювання така практика може призвести до зловживань і порушення основних свобод [40, с.31].

В Україні питання конфіденційності даних знаходиться в стадії активної адаптації до європейських норм, що зумовлює необхідність дотримання стандартів, які регулюють обробку персональних даних. Це законодавче врегулювання покликане забезпечити більшу прозорість у використанні технологій, але також накладає обмеження на їхнє впровадження. Наприклад, вимоги до отримання згоди користувачів на збір та обробку їхніх даних можуть ускладнити реалізацію деяких рішень, пов'язаних із безпекою. У разі відсутності чітких механізмів контролю за використанням даних, ризик неправомірного їх використання зростає, що може мати негативні наслідки як для користувачів, так і для самих організацій.

Отже, баланс між впровадженням новітніх технологій у сфері безпеки та захистом конфіденційності особистих даних є викликом для українського суспільства. Державні органи, підприємства та розробники технологій повинні працювати над створенням ефективних політик, які забезпечать не лише безпеку, а й дотримання прав людини. Без цього зростання технологій може призвести до нових форм кіберзлочинності, які експлуатують недоліки в системах захисту даних. У підсумку, новітні технології мають величезний потенціал у боротьбі з кіберзлочинністю, але їхнє використання повинно супроводжуватися відповідними етичними та правовими рамками [40, с.32].

Одним із серйозних викликів, які стоять перед кібербезпекою новітніх технологій, є захист самої інфраструктури, зокрема систем штучного інтелекту. Ці системи можуть бути вразливими до атак, які намагаються модифікувати алгоритми, змінюючи їхню поведінку та функціонування. Це створює ризик для навіть найнадійніших систем захисту, які можуть бути скомпрометовані, що, в свою чергу, загрожує безпеці важливих даних і інфраструктури. В Україні, де кіберзагрози виходять за межі внутрішніх загроз і мають зовнішні компоненти, проблема захисту алгоритмів стає особливо актуальною. Безпечність алгоритмів має прямий вплив на стабільність державних інформаційних систем, які обробляють чутливі дані громадян.

Крім того, одна з ключових проблем, що ускладнює ситуацію, — це нестача кваліфікованих фахівців у сфері кібербезпеки. Хоча IT-сектор в Україні розвивається швидкими темпами, кількість професіоналів, які спеціалізуються на кібербезпеці, залишається недостатньою. Це створює вразливість для державних і приватних структур, оскільки відсутність кваліфікованих кадрів знижує їх здатність адекватно реагувати на кіберзагрози. Державні ініціативи, спрямовані на підготовку фахівців у цій галузі, починають з'являтися, але їх реалізація вимагає часу та значних ресурсів [41, с.142].

Відсутність достатньої кількості фахівців з кібербезпеки не лише ускладнює інтеграцію новітніх технологій у бізнес-процеси, але й підриває загальний рівень безпеки країни. Для роботи з такими технологіями потрібен високий рівень експертизи та досвіду, які, на жаль, не завжди можна швидко набути. Таким чином, для успішного протистояння кіберзлочинності Україні необхідно не лише інвестувати в технології, але й у розвиток людських ресурсів у сфері кібербезпеки. Без цього побудова надійної і стійкої інфраструктури залишиться під загрозою, а ризики кіберзлочинності можуть зростати.

Проблеми співпраці між державним і приватним секторами становлять серйозну перешкоду для ефективної боротьби з кіберзлочинністю. Для успішної протидії цьому явищу необхідно об'єднати зусилля державних органів, бізнесу та громадських організацій, оскільки кожен з цих секторів має свої сильні сторони та ресурси, які можуть доповнювати один одного. Однак на практиці реалізація спільних ініціатив часто ускладнена, адже між державними структурами та приватними компаніями існують суттєві розбіжності в пріоритетах та можливостях [41, с.143].

Державні органи, як правило, стикаються з обмеженнями у фінансуванні, що ускладнює впровадження новітніх рішень у сфері кіберзахисту. Бюджетні обмеження можуть призводити до затримок у модернізації технологій, що, в свою чергу, знижує рівень безпеки на

державному рівні. У той же час, приватні компанії активно інвестують у кібербезпеку, прагнучи захистити свої активи та дані. Проте, незважаючи на свої ресурси, не завжди вони готові ділитися технологіями та досвідом з державними структурами. Це може бути зумовлено як комерційними інтересами, так і недовірою до державних органів, що заважає створенню конструктивного діалогу між секторами.

Важливо зазначити, що ефективна співпраця між державними та приватними структурами є ключовим фактором у протидії кіберзлочинності. Налагодження партнерських відносин може допомогти зменшити розрив у технологічному оснащенні, покращити обмін інформацією про загрози та найкращі практики, а також забезпечити більш комплексний підхід до захисту критичної інфраструктури. Для цього необхідно створити платформи для обміну даними, розробити спільні ініціативи та програми навчання, які сприятимуть інтеграції зусиль обох секторів. Тільки таким чином можливо досягти більшої ефективності у боротьбі з кіберзлочинністю, що стане гарантією безпеки не лише для державних інститутів, але й для приватних компаній і суспільства в цілому [42, с.18].

Законодавче врегулювання використання новітніх технологій у протидії кіберзлочинності є важливим аспектом, який потребує особливої уваги в Україні. Хоча українське законодавство поступово адаптується до європейських стандартів, воно все ще має численні прогалини та недоліки, які необхідно усунути для ефективного захисту прав громадян і забезпечення безпеки інформаційного середовища.

Однією з ключових проблем є недостатня адаптація законодавства у сфері захисту персональних даних і конфіденційної інформації до нових викликів, що виникають у зв’язку з розвитком технологій штучного інтелекту та аналізу великих даних. З розвитком цих технологій стає все складніше контролювати, як саме використовуються персональні дані, а також забезпечувати їхню безпеку. Тому Україні необхідно оновити законодавчу базу, щоб вона відповідала сучасним умовам та вимогам, що постають в

умовах цифровізації. Це включає розробку чітких норм щодо збору, обробки та зберігання даних, а також механізмів контролю за дотриманням цих норм.

Крім того, важливим аспектом є вдосконалення законодавства щодо відповідальності за кіберзлочини. Оскільки кіберзлочинність є глобальним викликом, Україні слід приділити особливу увагу питанням міжнародного співробітництва в цій сфері. Необхідно створити правову основу для спільних дій з іншими державами, щоб забезпечити ефективну боротьбу з кіберзлочинцями, які часто діють через кордони. Це може включати підписання міжнародних угод, обмін інформацією про загрози, а також спільні розслідування [43, с.121].

Попри всі складнощі, перспективи застосування новітніх технологій у протидії кіберзлочинності в Україні є значними. Активне використання ШІ, великих даних, блокчейну, біометричних систем, хмарних сервісів та інших технологій може значно підвищити ефективність боротьби з кіберзлочинністю. Успішне впровадження цих технологій вимагає комплексного підходу, що включає як технічні, так і організаційні заходи, а також широку міжсекторальну співпрацю.

Таким чином, інтеграція новітніх технологій у сферу кібербезпеки є як невід’ємною частиною захисту України в умовах сучасного світу, так і серйозним випробуванням для її суспільства та державних структур. Для досягнення успіху у боротьбі з кіберзлочинністю Україні потрібно забезпечити не лише технічне переоснащення, але й розвиток кадрового потенціалу, законодавчу підтримку та готовність до співпраці на всіх рівнях суспільства.

ВИСНОВКИ

У висновках до кваліфікаційної роботи на тему «Кіберзлочинність та виклики кібербезпеки для правоохоронних органів» підсумовано основні аспекти дослідження проблеми кіберзлочинності та розглядає можливості й виклики для правоохоронної системи у сфері кібербезпеки.

В роботі розкрито специфіку кіберзлочинності як одного з найсерйозніших викликів для сучасного суспільства, що охоплює не лише зловмисні дії в інтернеті, але й систематичні атаки на інформаційні ресурси різних державних і приватних установ. Проблема кіберзлочинності виявилася вкрай комплексною, оскільки включає широке коло різновидів злочинів — від шахрайства й крадіжок даних до кібершпигунства та інформаційного тероризму.

Поняття кіберзлочинності об’єднує ряд дій, що порушують безпеку інформаційних ресурсів, цілісність даних та конфіденційність інформації. У ході дослідження виявлено, що кіберзлочинність характеризується високим рівнем організації та часто пов’язана з використанням передових технологій. Дослідження дозволило розкрити основні різновиди кіберзлочинності, зокрема фінансові махінації, атаки на приватні дані, шкідливе програмне забезпечення та деструктивні дії проти критичної інфраструктури. Така розмаїтість злочинних дій вимагає специфічних підходів у їх виявленні та розслідуванні.

Окрім різновидів кіберзлочинності, у роботі також розглянуто методи та засоби, які використовують кіберзлочинці. Зокрема, було визначено, що найбільш розповсюдженими методами є фішинг, соціальна інженерія, DDoS-атаки, експлойти та шкідливі програми різних видів, включаючи віруси, трояни, і руткіти. Використання таких методів вимагає від правоохоронців не тільки знань про технічні особливості атак, але й розуміння людського фактору, що може допомогти у виявленні слабких місць у системах безпеки.

Таким чином, необхідність впровадження технологічної обізнаності серед персоналу правоохоронних органів стала ще більш очевидною.

Міжнародний та національний контексти боротьби з кіберзлочинністю відіграють ключову роль у ефективності протидії кіберзлочинам. Аналіз міжнародного права показав, що сьогодні існує кілька універсальних механізмів, таких як Будапештська конвенція про кіберзлочинність, які є зразком для розробки національних стратегій. Однак попри ці зусилля, глобальна правова база все ще має багато прогалин, особливо у випадках, коли йдеться про юрисдикцію та міжнародну співпрацю. Правоохоронні органи країн, включаючи Україну, стикаються зі складнощами у застосуванні єдиних стандартів у боротьбі з кіберзлочинністю, що часто призводить до проблем у розслідуванні транскордонних злочинів.

Дослідження показало, що загрози кібербезпеці з кожним роком зростають, і їх вплив на правоохоронні органи є значним. Зокрема, новітні загрози, такі як атаки на критичну інфраструктуру, кібершпигунство, ймовірність використання штучного інтелекту у злочинних цілях, ускладнюють роботу правоохоронців, які повинні швидко адаптуватися до нових викликів. Це також вимагає значних фінансових та технічних ресурсів, а також оновлення методів, використовуваних для розслідування кіберзлочинів.

Захист від кіберзлочинності потребує ефективних та інноваційних підходів. У рамках дослідження були проаналізовані методи, що використовуються як на міжнародному рівні, так і в Україні, зокрема кіберполіція, спеціалізовані аналітичні центри та система швидкого реагування на кіберзагрози. Міжнародний досвід показує, що міжвідомча кооперація, обмін даними, розвиток інформаційних платформ для правоохоронних органів, такі як Інтерпол, Європол та ENISA, допомагають значно підвищити ефективність боротьби з кіберзлочинністю. Українська практика, хоч і поступово наближається до європейських стандартів, все ще

має простір для вдосконалення, зокрема у сферах технічного оснащення та навчання кадрів.

Важливою частиною дослідження стало вивчення перспектив та проблем, пов’язаних із використанням новітніх технологій у боротьбі з кіберзлочинністю. Такі технології, як штучний інтелект, машинне навчання, блокчейн, стають не лише корисними інструментами для правоохоронних органів, але й створюють нові загрози, оскільки вони також можуть бути використані злочинцями. Отже, існує потреба у постійному аналізі та вдосконаленні технологічної бази правоохоронних органів для випередження злочинців у кіберпросторі.

В цілому, результати роботи свідчать про те, що кіберзлочинність є динамічним явищем, яке постійно адаптується до нових технологій і соціальних умов. Це вимагає від правоохоронних органів гнучкості, технологічної підготовленості та спроможності до співпраці на міжнародному рівні. Подальше вдосконалення законодавства, підвищення обізнаності про кіберзагрози серед населення, а також активне впровадження нових технологій у протидії кіберзлочинності є важливими завданнями, які потребують уваги.

Таким чином, дослідження дозволяє зробити висновок, що ефективна боротьба з кіберзлочинністю можлива лише за умов синергетичної роботи державних структур, приватного сектору та міжнародного співтовариства. Правоохоронні органи повинні впроваджувати нові підходи та оновлювати свої технічні засоби, щоб відповідати вимогам сучасності й забезпечувати безпеку інформаційного простору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Підручник. В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. Київ: ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.

2. Кіберкультура та кібербезпека в умовах війни: психологічний практикум: практичний посібник / Юлія Чаплінська ; Національна академія педагогічних наук України, Інститут соціальної та політичної психології. Київ, 2023. 80 с.

3. Кузьменко Б.В., Заіка Ю.О. Кібертероризм: світові й українські реалії. *Науковий вісник Академії внутрішніх справ*. 2012. № 2(81). С. 92-98.

4. Бистрова Б. Рівні забезпечення якості підготовки фахівців з кібербезпеки в закладах вищої освіти США. П*едагогічні науки: теорія, історія, інноваційні технології.* 2019. № 2 (86). С.140-149.

5. Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. Інформаційна безпека: соціально-правові аспекти: підручник; за заг.ред. Скулиша Є.Д.. 2010. 512 с.

6. Даник Ю. Г., Телелим В. М., Чмельов В. О. Основні аспекти стратегії превентивної оборони та її реалізації. *Наука і оборона*. 2010. № 2. С. 15–23.

7. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. К., 2023. №9 (вересень). 351 с.

8. Баранова, О. А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*, 2(42), 2014. С. 54–62.

9. Биков, В. Ю., Буров, О. Ю., & Дементієвська, Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання*, Т. 70, №2, 2019. С. 313–331.

10. Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Навч. посіб. К.: Видавництво Ліра-К, 2023. 484 с.

11. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Г.М. Гулак. К.: Видавництво НА СБ України, 2020. 256 с.

12. Кібервійни, кібертероризм, кіберзлочинність. Концепції, стратегії, технології, Когут Ю. К.: Видавництво Сідкон, 2022. 284 с.

13. Кібербезпека в Україні: нормативна база, коментарі та роз'яснення, актуальна судова практика, Пєтков С.В., Журавльов Д.В., Дрозд О.Ю., Дрозд В.Г. К: Видавництво ЦУЛ, 2022. 460 с.

14. Газізова, Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. Юрист і Закон (ТОВ «ЛІГА ЗАКОН»), № 45. 2022. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606# (дата звернення 18.10.2024 р.)

15. Горбенко, В. І. Курс «Кібервійни та кібербезпека в сучасному світі» [Lecture notes]. Система електронного забезпечення навчання ЗНУ. https://moodle.znu.edu.ua/course/view.php?id=6844 (дата звернення 18.10.2024 р.)

16. Забезпечення інформаційної безпеки держави: Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.

17. Климчук О. О. Забезпечення інформаційної безпеки у провідних країнах світу : навч. посіб. О. О. Климчук, Д. С. Мельник, В. М. Панченко, В. М. Петрик та ін.; за заг. ред. В. М. Петрика. Київ : Вид-во ІСЗЗІ НТУУ «КПІ», 2014. 260 с.

18. Онищенко С., Глушко А. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Economic security of the state and economic entities.* Економіка і регіон. Національний університет ім. Юрія Кондратюка. № 1 (84). 2022 р. С. 13–20.

19. Які російські та проросійські хакери атакують Україну. Державна служба спеціального зв'язку та захисту інформації України. Д*ержавні сайти України.* URL : https://cip.gov.ua/ua/news/yaki-rosiiski-ta-prorosiiski-khakeri-atakuyut-ukrayinu. (дата звернення 18.10.2024 р.)

20. АрміяInform. У ЗСУ фактично вже є кібервійська, вони реально працюють – Олег Гайдук. URL : https://armyinform.com.ua/2022/11/22/u-zsu-faktychno-vzhe-ye-kibervijska-vony-realno-praczyuyut-oleg-gajduk/. (дата звернення 18.10.2024 р.)

21. Тімкін І.Ф., Новікова Н.Є. Структурно-функціональна характеристика системи забезпечення національної безпеки України. URL: er.nau.edu.ua. (дата звернення 18.01.2024 р.)

22. The Village Україна. В Україні узаконять процедуру Bug Bounty та створять посаду офіцера з кібербезпеки. URL : https://www.the-village. com.ua/village/city/city-news/321781-v-ukrayini-uzakonyat-protseduru-bug-bounty-i-stvoryat-posadu-ofitsera-z-kiberbezpeki?from=readmore. (дата звернення 18.01.2024 р.)

23. Даник Ю. Г., Супрунов Ю. М. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України. *Проблеми створення, випробування та експлуатації складних інформаційних систем*: збірник наукових праць. Житомир : ЖВІНАУ. 2011. Вип. 5. С. 5–22.

24. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–169.

25. Ширяєв Д.О. Кібербезпека та сучасний світ. *Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів*. Вінниця, 2023. С. 600–602.

26. Бєлкін Л.М., Юринець Ю.Л., Бєлкін М.Л., Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020–2021 років.

Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law», 3(64). 2022. С. 78–86.

27. Яковлєв П. Державне регулювання у сфері захисту кіберпростору як складник забезпечення інформаційної безпеки України. *Customs Scientific Journal*. 2020. № 1. С. 43–48.

28. Шестак Я. І. Кібергігієна у інформаційному просторі в умовах воєнного стану. *Інформаційна безпека та комп'ютерні технології*. Ценральноукраїнський національний технічний університет, Кропивницький, 2022. С. 5–6.

29. Климчук О. О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави*. 2015. № 3. С. 75–83.

30. Maennel K., Mäses S., Maennel O. Cyber Hygiene: The Big Picture. *Lecture Notes in Computer Science*. 11252 LNCS. 2018. pp. 291-305.

31. Gupta S., Furnell S. From Cybersecurity Hygiene to Cyber Well-Being. *Lecture Notes in Computer Science*. 13333. 2022. pp. 124-134.

32. Vishwanath A., Neo L. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*. 2020. pp. 128.

33. Захист інформації та кібербезпека в електронних комунікаційних мережах: навч. посіб. П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2023. 188 с.

34. Баранов О. А. Інтернет речей (IoT) і блокчейн. *Інформація і право.* № 1(24)/2018. С. 59−71.

35. Довгань О. Д. Ткачук Т. Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. 2019. № 1. С. 86−100.

36. Кубанов Є. В. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління. *Аспекти публічного правління*. Том 6, № 8. 2018. С. 49−55.

37. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 422 с.

38. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162−169.

39. Присяжнюк М. М. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка.* Військово-спеціальні науки. 2013. Вип. 30. С. 42−46.

40. Цимбалюк В. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* Науково-технічний збірник. Київ, 2004. С. 30−33.

41. Ткачук Т. Ю. Кібербезпека: підходи до визначення в окремих країнах. *Актуальні проблеми управління інформ. безпекою держави*: мат. наук.-практ. конф. (Київ, НА СБ України. 24.05.17). 2017. С. 142–144.

42. Брижко В. М. Філософія права: герменевтика в сфері інформаційного права. *Правова інформатика*. 2014. № 1(41). С. 18−22.

43. Ланде Д. В., Фурашев В. М. Основи інформаційного і соціально-правового моделювання: монографія. Київ: ТОВ «ПанТот», 2012. 144 с.